APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/270,967	03/17/1999	DAVID GRABELSKY	98630	3345

20306   7590   04/29/2003

MCDONNELL BOEHNEN HULBERT & BERGHOFF
300 SOUTH WACKER DRIVE
SUITE 3200
CHICAGO, IL   60606

EXAMINER
NOBAHAR, ABDULHAKIM

ART UNIT	PAPER NUMBER
2132	

DATE MAILED: 04/29/2003

16

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 07-01)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

    A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☐ Responsive to communication(s) filed on _____ .

2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-39_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-39_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved by the Examiner.

    If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

      1. ☐ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

    a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 4,5,6,8   6) ☐ Other: .
10,11,13,14,15

DETAILED ACTION

Double Patenting

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

Claims 1-39 are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-20 of copending Application No. 09/384158. Although the conflicting claims are not identical, they are not patentably distinct from each other because the conflicting claims of the copending application are broader than the claims of this application. The claims of this application expressly specify that the security values, the security certificate and the ports are allocated to the devices on the local network by the router on the local network.

This is a <u>provisional</u> obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

Claims 1-3, 6-10, 14-15, 18, 20-25, 28-29, 31 and 34-37 are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1-42 of U.S. Patent No. 6,353,614. Although the conflicting claims are not identical, they are not patentably distinct from each other because the conflicting claims of this application are broader than the claims 1-42 of the U.S. patent No. 6,353,614. These claims do not expressly specify the use of a Port Allocation Protocol invalidate message for de-allocating the unique port numbers allocated to a network device.

Information Disclosure Statement

The information disclosure statements filed on August 22, 2000 and June 3, 2002 fail to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each U.S. and foreign patent; each publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. They have been placed in the application file, but the information referred to therein do not contain the referenced documents listed below, thus the missing documents have not been considered.

IDS	Referenced Documents
August 22, 2000	International Search Report for PCT/US00/07057, Dated August 9, 2000
June 3, 2002	Numbers 36 and 52 from the list of documents

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 8, 20, 24-26 and 36 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Referring to claim 8, 20, 24-26 and 36, these claims are rejected for lack of antecedent bases for the following matters:

Claim 8 for "the locally unique ports"

Claim 20, last line for "the locally unique ports"

Claim 24, first line for "the local network address" and on second line for "the virtual tunnel header"

Claim 25, first line for "the first protocol"

Claim 26, first line for "the Internet Protocol security protocol"

Claim 36, fifth line for "the second network device", on eleventh line for "the network device" and twelfth line for "to first network device"

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the
United States before the invention thereof by the applicant for patent, or on an international application
by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this
title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act

of 1999 (AIPA) do not apply to the examination of this application as the application

being examined was not (1) filed on or after November 29, 2000, or (2) voluntarily

published under 35 U.S.C. 122(b). Therefore, this application is examined under 35

U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-33 are rejected under 35 U.S.C. 102(e) as being anticipated by Ylonen

et al. (6,438,612 B1) (hereinafter Ylonen).

Referring to claims 1 and 9, Ylonen discloses:

"A method for distributed network address translation with security, comprising

the following steps:

Requesting from a first network device on a first computer network with a first

protocol, one or more locally unique security values from a second network device on

the first computer network to uniquely identify the first network device during secure

communications with a third network device on a second external network and for

distributed network address translation with security;

Receiving the one or more locally unique security values on the first network device from the second network device with the first protocol;

Storing the one or more locally unique security values on the first network device, wherein the one or more locally unique security values are used to create a secure virtual connection for secure communications with the third network device and for distributed network address translation;

Receiving a request message with a first protocol on a second network device for one or more locally unique security values from a first network device; allocating one of more locally unique security values on the second network device;

Storing a network address for the first network device with the one or more locally unique security values in a table associated with the second network device, wherein the table is used to maintain a mapping between a network device and one or more locally unique security values for distributed network address translation; and

Sending the one or more locally unique security values in a response message with the first protocol to the first network device." See abstract, col. 1, lines 32-40, col. 2, lines 60-67, col. 3, line 49-col. 4, 16, col. 5, lines 61-col. 6, line 5, col. 7, lines 6-17 and lines 46-55, col. 8, lines 44-67 and col. 9, lines 33-67.

Referring to claims 2 and 10, Ylonen discloses:

"A computer readable medium having stored therein instructions for causing a central processing unit to execute the Method of Claims 1 and 9." See col. 15, lines 38-48.

Referring to claims 3 and 11, Ylonen discloses:

"The method of Claims 1 and 9 wherein the second network device is a distributed network address translation router." See col. 1, lines 12-20.

Referring to claims 4 and 12, Ylonen discloses:

"The method of Claims 1 and 9 wherein the one or more locally unique security values are one or more security parameter indexes for an Internet Protocol security protocol." See col. 3, lines 16-31.

Referring to claims 5 and 13, Ylonen discloses:

"The method of Claims 4 and 10 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol or an Internet Key Exchange protocol." See col. 3, lines 16-31 and col. 4, lines 39-50.

Referring to claim 6 Ylonen, discloses:

"The method of Claim 1 wherein the first protocol is a Port Allocation Protocol." See col. 8, lines 20-27.

Referring to claim 7, Ylonen discloses:

"The method of Claim 1 wherein the requesting step further includes requesting one or more locally unique ports used to uniquely identify the first network device on the

first network for distributed network address translation." See col. 2, lines 6-10 and col.

6, lines 6-13.

Referring to claim 8, Ylonen discloses:

"The method of Claim 1 wherein the locally unique ports are Port Allocation

Protocol ports." See col. 2, lines 6-10, col. 6, lines 6-13 and col. 8, lines 20-27.

Referring to claims 14 and 20, Ylonen discloses:

"A method for distributed network address translation using security, comprising

the following steps:

Receiving a first message in a second secure protocol on a first network device on a

first network to establish a secure virtual connection to the first network device from a

third network device on a second external network;

Selecting a locally unique security value to use for the secure virtual connection

from a list of locally unique security values, wherein the list of locally unique security

values was received from a second network device on the first network with a first

protocol;

Sending a second message with second secure protocol to establish a secure

virtual connection to the first network device on the first network from the third network

device on the second external network wherein the second message includes the

selected locally unique security value and security certificate sent to the first network

device by the second network device;

Sending a request message in a second secure protocol from a first network device on a first network to a second network device on the first network, wherein the request message in the second secure protocol includes security information;

Routing the request message from the second network device to a third network device on a second external network over a secure virtual connection between the first network device and the third network device;

Receiving a reply message in the second secure protocol from the third network device on the second network device on the first network for the first network device, wherein the reply message in the second secure protocol includes security information from the request message allocated by the second network device; and

Routing the reply message from the second network device to the first network device on the first network using the locally unique ports used for distributed network address translation." See abstract, col. 1, lines 12-40, col. 3, line 49-col. 4, 16, col. 5, lines 61-col. 6, line 5, col. 7, lines 6-17, col. 8, lines 44-67, col. 9, lines 33-67 and col. 11, lines 42-64.

Referring to claims 15 and 21, Ylonen discloses:

"A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claims 14 and 20." See col. 15, lines 38-48.

Referring to claim 16, Ylonen discloses:

"The method of Claim 14 wherein the list of one or more locally unique security values is a list of one or more security parameter indexes for Internet Protocol security protocol." See col. 3, lines 16-31.

Referring to claims 17 and 26, Ylonen discloses:

"The method of Claim 14 wherein the Internet Protocol security protocol is any of an Authentication Header protocol, Encapsulated Security Payload protocol, or an Internet Key Exchange Protocol." See col. 3, lines 16-31 and col. 4, lines 39-50.

Referring to claims 18 and 25, Ylonen discloses:

"The method of Claim 14 wherein the first protocol is a Port Allocation Protocol and the second secure protocol is an Internet Protocol security protocol." See col. 3, lines 16-31 and col. 8, lines 20-27.

Referring to claim19, Ylonen discloses:

"The method of Claim 14 wherein the secure virtual connection is an Internet Protocol security protocol security association." See col. 1, lines 48-57, col. 6, lines 6-13 and col. 7, lines 51-60.

Referring to claim 22, Ylonen discloses:

"The method of Claim 20 wherein the step of sending a request message in a second 5 secure protocol includes:

Constructing a virtual tunnel header for a local network address determined for the second network device;

Prepending the virtual tunnel header to the request message, wherein the virtual tunnel header is used to create a virtual tunnel between the first network device and the second network device;

Sending the request message to the second network device from the first network device over the virtual tunnel." See col. 2, 17-43, and line 60-col. 3, line 15, col. 3, lines 49-56 and col. 5, lines 56-67.

Referring to claim 23 Ylonen discloses:

"The method of Claim 20 wherein the step of routing the reply from the second network device to the first network device on the first network using the locally unique port from the reply in the second secure protocol includes:

Determining a local network address for the first network device using the locally unique port associated with the second network device;

Constructing a virtual tunnel header for the determined local network address for the first network device;

Prepending the virtual tunnel header to the reply message, wherein the virtual tunnel header is used to create a virtual tunnel between the second network device and the first network device; and

Forwarding the reply message to the first network device from the second network device over the virtual tunnel." See col. 1, lines 50-58, col. 2, lines 6-50 and col. 11, lines 4-60.

Referring to claim 24, Ylonen discloses:

"The method of Claim 20 wherein the local network address is an Internet Protocol address and the virtual tunnel header is an Internet Protocol tunnel header." See col. 1, lines 48-57, col. 2, lines 35-52, col. 6, lines 6-13 and col. 7, lines 51-60.

Referring to claim 27, Ylonen discloses:

"The method of Claim 20 wherein the security information includes any of a locally unique security value or a security certificate." See col. 1, lines 26-40 and col. 2, lines 6-16.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 28-39 are rejected under 35 USC 103(a) as being unpatentable over

Ylonen et al (6,438,612 B1) (hereinafter Ylonen) in view of Danieli (6,510,513 B1).

Referring to claims 28, 34 and 36, Ylonen teaches:

"Requesting one or more locally unique ports with a first message from a first

protocol on a first network device from a second network device, wherein the one or

more locally unique ports are used for distributed network address translation;

Requesting one or more locally unique security values with a first message from

the first protocol from the second network device, wherein the one or more locally

unique security values are used with a second secure protocol to establish a secure

virtual connection between the first network device and a third network device on a

second external computer network and are used for distributed network address

translation with security;

Sending one or more locally unique ports allocated on a second network device

on a first computer network to a first network device on the first computer network with a

second message from a first protocol wherein the one or more locally unique ports are

used for distributed network address translator;

Sending one or more locally unique security values allocated on the second

network device to the first network device with a second message from the first protocol

wherein the one or more locally unique security values are used with a second secure

protocol to establish a secure virtual connection between the first network device and a

third network device on a second external computer network and are used for

distributed network address translation with security;

A routing network device for allocating one or more locally unique ports, one or

more locally unique security values and security certificates used for distributed network

address translation with security for a plurality of other network devices, wherein the

second network device provides local security certificate services and routing services

for distributed network address translation with security; and

A network address table associated with the routing network device for mapping

one or more locally unique security values to a network address for a network device."

See abstract, col. 1, lines 32-40, col. 2, lines 60-67, col. 3, line 49-col. 4, 16, col. 5, lines

61-col. 6, line 5, col. 7, lines 6-17 and lines 46-55, col. 8, lines 44-67 and col. 9, lines

33-67.

However, Ylonen does not teach the use of a security certificate to be provided to

a requesting network device from the router for associating an encryption key with other

information related to the network device. Danieli teaches:

"Requesting a security certificate on the first network device from the second

network device, wherein the security certificate includes a binding between a public

encryption key and a combination of a network address for the first network device and

the one or more locally unique ports and the second network device provides local

security certificate services;

Sending a security certificate created on the second network device to the first

network device, wherein the second network device provides local security certificate

services on the first computer network and wherein the security certificate includes a binding for a public encryption key for the first network device and a combination of a network address for the first network device and the one or more locally unique ports allocated to the first network device to authenticate an identity for the first network device for a secure virtual connection between the first network device and a third network device on a second external computer network;

A security certificate for binding a public encryption key for a network device and a combination of a network address for the network device and one or more locally unique ports allocated to first network device by the routing network device to authenticate an identity for the network device for a secure virtual connection with external network device on an external computer network, wherein the security certificate is issued by a second network device providing local security certificate services for distributed network address translation with security." See col. 1, lines 44-62, col. 2, lines 42-65, col. 5, lines 50-61, col. 7, lines 6-27, col. 8, lines 28-33 and col. 11, lines 48-62.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to incorporate the use of a security certificate to be provided to the communicating network device by the router as taught in Danieli with the method of Ylonen because it would provide for a mechanism to guarantee the authenticity and validity of electronic data (col. 2, lines 31-35).

Referring to claims 29 and 35, Ylonen discloses:

"A computer readable medium having stored therein instructions for causing a central processing unit to execute the method of Claims 28 and 34." See col. 15, lines 38-48.

Referring to claims 30 and 38, Ylonen discloses:

"The method of Claims 28 and 36 wherein the one or more locally unique security values are security parameter indexes from an Internet Protocol security protocol." See col. 3, lines 16-31.

Referring to claims 31 and 37, Ylonen discloses:

"The method of Claims 28 and 37 wherein the second network device is a distributed network address translation router." See col. 1, lines 12-20.

Referring to claim 32, Ylonen discloses:

"The method of Claim 28 further comprising:

Establishing a secure virtual connection between the first network device and the third network device on the second external network using the security certificate." See col. 1, 50-58 and col. 4, lines24-38.

Referring to claims 33 and 39, Ylonen discloses:

"The method of Claims 32 and 36, wherein the secure virtual connection is an

Internet Protocol security protocol security association." See col. 1, lines 48-57, col. 6,

lines 6-13 and col. 7, lines 51-60.

Conclusion

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-

305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers

for the organization where this application or proceeding is assigned are 703-746-7239

for regular communications and 703-746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or

proceeding should be directed to the receptionist whose telephone number is 703-305-

3900.

                                            Abdulhakim Nobahar
                                            Examiner
                                            Art Unit 2132

April 25, 2003

                                            GILBERTO BARRON
                                            SUPERVISORY PATENT EXAMINER
                                            TECHNOLOGY CENTER 2100